Kaveh S. Elihu, Esq. (SBN 268249)
Saima Ali Gipson, Esq. (SBN 324752)
EMPLOYEE JUSTICE LEGAL GROUP, PC
1001 Wilshire Boulevard
Los Angeles, California 90017
Telephone: (213) 382-2222
Facsimile: (213) 382-2230
Email: kelihu@ejlglaw.com
sali@ejlglaw.com

Attorneys for Plaintiff,
Carlos Malacon

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

CARLOS MALACON, an individually, and on behalf of all similarly situated individuals, Plaintiff, v. VERIZON COMMUNICATIONS, INC., a Delaware corporation; and DOES 1 through 50, inclusive, Defendants.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Carlos Malacon ("Plaintiff") individually and on behalf of all other similarly situated, brings this action against Defendant Verizon Communications, Inc. ("Defendant") based on personal knowledge and the investigation of counsel, and allege as follows:

INTRODUCTION

1. With this action, Plaintiff seeks to hold Defendant responsible for the harms caused to Plaintiff and other similarly situated persons ("Class" or "Class Members" or "Breach Victims") in a massive and preventable data breach of Defendant's inadequately protected computer network.

2. Defendant revealed in a February 7, 2024 notification to the Maine Attorney General that a Verizon employee gained unauthorized access to a file

containing sensitive employee information on September 21, 2023 (the "Data Breach" or "Breach").

3. Defendant did not discover the Data Breach until December 21, 2023, nearly three months later.

4. Further, Defendant determined that the Data Breach contained sensitive personal information ("Personal Information"), including full names, physical addresses, dates of births, Social Security numbers, national identification, gender, union affiliation, and compensation information of Plaintiff and Breach Victims.

5. The Personal Information for 63,000 Verizon employees, including Plaintiff, was affected by this Data Breach.

6. In short, thanks to Defendant's failure to protect the Breach Victims' Personal Information, cybercriminals were able to steal everything they could possibly need to commit nearly every conceivable form of identity theft and wreak havoc on the financial and personal lives of potentially millions of individuals.

7. Defendant is a multinational telecommunications conglomerate that is incorporated in Delaware and headquartered in New York.

8. Defendant's conduct – failing to implement adequate and reasonable measures to ensure their electronic systems were protected, failing to take adequate steps to prevent and stop the Data breach, and failing to timely detect the breach, failing to disclose the material facts that they did not have adequate electronic systems and security practices to safeguard the Personal Information, failing to honor their duty to protect the Breach Victims' Personal Identities, and failing to provide timely and adequate notice of the Data Breach – caused substantial harm and injuries to Plaintiff and the Breach Victims.

9. As a result of the Data Brach, Plaintiff and the Breach Victims have suffered damages. Now that their Personal Information has been hacked, Plaintiff and Breach Victims are at imminent risk of identity theft. And this will continue, as

they must spend their time being extra vigilant, due to Defendant's failures, to try to prevent being victimized for the rest of their lives.

10. Plaintiff brings this class action lawsuit on behalf of a nationwide and statewide class to hold Defendant responsible for its negligent and reckless failure to use reasonable, current cybersecurity measures to protect class members' Personal Information.

11. Because Defendant presented such a soft target to cybercriminals, Plaintiff and Breach Victims have already been subjected to violations of their privacy, fraud, and identity theft, or have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Breach Victims must now and in the future, spend time to more closely monitor their credit reports, financial accounts, phone lists, and online accounts to guard against identity theft.

12. Plaintiff and Breach Victims may also incur out-of-pocket costs for, among other things, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identify theft.

13. On behalf of himself and the Breach Victims, Plaintiff seeks actual damages, statutory damages, and punitive damages, with attorney fees, costs, and expenses under negligence, negligence per se, breach of fiduciary duties, breach of confidence, breach of implied contract, and invasion of privacy. Plaintiff also seeks injunctive relief, including significant improvements to Defendant's data security systems, future annual audits, and long-term credit monitoring services funded by Defendant, and other remedies as the Court sees fit.

THE PARTIES

11. Plaintiff Carlos Malacon is a citizen of California, currently residing in South Gate, California.

12. Defendant Verizon Communications, Inc. is a Delaware corporation based in Manhattan, New York.

13. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this Complaint to reflect their true names and capacities of such other responsible parties when their identities become known.

14. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

15. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

16. Defendant is a Delaware Corporation with its principal place of business in Manhattan, New York.

17. Jurisdiction is proper under 28 U.S.C. § 1332(d)(2) because Plaintiffs are not all residents of California and further seek relief on behalf of a Class, which will result in at least one class member belonging to a different state than that of Defendant.

18. Additionally, Plaintiffs are seeking damages for a nationwide and statewide Class that will exceed the $5,000,000.00 threshold for federal court jurisdiction. Therefore, both diversity jurisdiction and the damages threshold under the Class Action Fairness Act of 2005 ("CAFA") are present, and this Court has jurisdiction.

19. Venue is proper in this district pursuant to 28 U.S.C. § 1391 because Defendant operates, resides and has its principal place of business in this district, and a substantial part of the events or omissions giving rise to the claims occurred in this district.

/ / /

/ / /

FACTUAL ALLEGATIONS

20. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

21. Plaintiff was employed by Defendant from approximately April 2021 to January 2024 as a Senior Business Account Manager.

22. On February 7, 2024, Defendant submitted a notice with the Office of the Attorney General in Maine ("Maine Notice") that a Data Breach occurred that resulted in the theft of sensitive information on September 21, 2023, but was not discovered until December 12, 2023.[1]

23. Defendant also reported in the Maine Notice that 63,206 persons were affected by this Data Breach nationwide.

24. Also on February 7, 2024, Defendant sent letters to Plaintiff and other Breach Victims informing them that, it detected an unauthorized user, another Verizon employee, had gained access to their electronic systems between September 21, 2023 ("Notice of Breach" or "Notice"). The Notice also informed Plaintiff and Breach Victim that Defendant conducted a review of the relevant file that was involved in the Breach and determined that the file may include Plaintiff's and Breach Victim's Personal Information.

25. Despite detecting the breach in December 2023, and knowing many Plaintiff and Class Members were in danger, Defendant did nothing to warn Breach Victims until another nearly two months later. During this time, the cyber criminals had free reign to surveil and defraud their unsuspecting victims.

26. In spite of the severity of the Data Breach, Defendant has done very little to protect Breach Victims. Defendant is only offering two years of credit monitoring and identity theft protection services.

[1] Data Breach Notifications, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/65b9290a-b22e-4ae7-93e7-5acb84357297.shtml

27. Defendant failed to adequately safeguard Breach Victims' Personal Information, allowing cyber criminals to access this wealth of priceless information for nearly five months before Defendant warned the Breach Victims to be on the lookout.

28. Defendant had an obligation created by reasonable industry standards, common law, and its representations to Breach Victims, to keep their Personal Information confidential and to protect the information from unauthorized access.

29. Plaintiff and Breach Victims provided their Personal Information to Defendant with the reasonable expectations and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

30. Because the Data Breach was an intentional hack by cyber criminals seeking information of value that they could exploit, Breach Victims are at imminent risk of severe identity theft and exploitation.

31. Plaintiff is very careful about not sharing her sensitive Personal Information. She has never knowingly transmitted unencrypted sensitive Personal Information over the internet or any other unsecured source.

32. Plaintiff stores any document containing her Personal Information in safe and secure locations or destroys such documents. He diligently chooses unique usernames and passwords for his various online accounts.

33. Since the Data Breach, Plaintiff has received an influx of spam telephone calls and messages.

34. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Personal Information, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

35. Plaintiff has a continuing interest in ensuring that his Personal Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

36. Defendant collects, maintains, and stores the Personal Information of Plaintiff and the Breach Victims in the usual course of business, as the Breach Victims were Defendant's own employees.

37. As an employer, Defendant is required by federal and state laws and regulations to protect Plaintiff's and Class Members' Personal Information.

38. In addition to its obligations under federal and state laws, Defendant owed a duty to its employees, the Breach Victims who Personal Information was entrusted to Defendant to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information in its possession from being compromised, lost stolen, accesses, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Breach Victims to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its electronic systems and networks, and the personnel responsible for them, adequately protected the Personal Information of the Plaintiff and Breach Victims.

39. Further, Defendant had a duty to train its personnel in exercising reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information of other employees.

40. Defendant owed a duty to Plaintiff and the Breach Victims whose Personal Information was entrusted to Defendant to design, maintain, and test its computer and electronic systems and email systems to ensure that Personal Information in Defendant's possession was adequately secured and protected.

41. Defendant owed a duty to Plaintiff and the Breach Victims whose Personal Information was entrusted to Defendant to create and implement

reasonable data security practices and procedures to protect the Personal Information in their possession, including adequately training its employees and others who accessed Personal Information within its computer systems on how to adequately protect Personal Information.

42. Defendant owed a duty to Plaintiff and the Breach Victims whose Personal Information was entrusted to Defendant to implement processes that would detect a breach on its data security systems in a timely manner.

43. Defendant owed a duty to Plaintiff and the Breach Victims whose Personal Information was entrusted to Defendant to act upon data security warnings and alerts in a timely fashion.

44. Defendant owed a duty to Plaintiff and the Breach Victims whose Personal Information was entrusted to Defendant to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Personal Information from theft because such an inadequacy would be a material fact in the decision to entrust Personal Information with Defendant.

45. Defendant owed a duty to Plaintiff and the Breach Victims whose Personal Information was entrusted to Defendant to disclose in a timely and accurate manner when data breaches occurred.

46. Defendant owed a duty of care to Plaintiff and the Breach Victims because they were foreseeable and probable victims of any inadequate data security practices.

47. Defendant knew or should have known that Defendant's computer and/or electronic systems were a target for cybersecurity attacks because warnings were readily available and accessible via the Internet.

48. Moreover, this is not the first time Defendant's employees have become victims of unauthorized access to their Personal Information. In May 2022, Defendant faced another data breach of its employees' Personal Information where a

hacker gained access to, collected and held ransom internal contact information and additional details, like names, ID numbers, phone numbers, and email addresses, of Defendant's employees.[2]

49. Defendant has faced at least seven instances of data breaches between 2008 and 2024.[3] As such, Defendant knew or should have taken measure to protect the Personal Information of the Breach Victims.

50. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[4] Cyber criminals can leverage Plaintiff's and Breach Victims' Personal Information that was stolen in the Data Breach to commit numerous additional crimes, including opening new financial accounts in Breach Victims' names, taking out loans in Breach Victims' names, using Breach Victims' names to obtain government benefits, using Breach Victims' Personal Information to file fraudulent tax returns using Breach Victims' information, obtaining driver's licenses in Breach Victims' names but with another person's photograph, and giving false information to police during an arrest. Even worse, Breach Victims could be arrested for crimes identity thieves have committed.

51. Personal Information is like currency today. It is an extremely valuable commodity to identify thieves that once the information has been compromised, criminals often trade the information on the cyber black-market for years.

52. Today, a person's personal information can be worth more than $1,000 on the dark web. Online banking login information costs on average $100, and $150 if the bank account has a minimum of $100 in the account.[5] Full credit card

---

[2] Shair, Umair, Hacker accesses a Verizon employee database and tries to ransom the data for $250,000, The Verge (May 22, 2022), https://www.theverge.com/2022/5/27/23144418/hacker-verizon-employee-database

[3] Reed, Catherine, Verizon Data Breaches: Full Timeline Through 2024, Firewall Times (February 20, 2024), https://firewalltimes.com/verizon-data-breaches/

[4] Facts + Statistics: Identity Theft and Cybercrime, Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

[5] Smith, Ryan, Revealed – how much is personal information worth on the dark web, Insurance Business (May 1, 2023), https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-

details and associated data costs between $10 and $100.[6] A high-Hackquality US driver's license with stolen identity information on it costs about $500.[7] A full range of documents and information on a person that will allow identity theft can be purchased for about $1,000.[8]

53. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

54. This Data Breach has and will lead to further devastating financial and personal losses to Breach Victims.

55. This is not speculative, as the Federal Trade Commission has reported that if hackers get access to Personal Information, they ***will*** use it.[9]

56. Plaintiff and the Breach Victims have experienced one or more of these harms as a result of the Data Breach.

57. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[10]

58. Defendant's offer of two year of credit monitoring to Plaintiff and the Breach Victims is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. Furthermore, credit monitoring only alerts someone to the fact

---

444453.aspx#:~:text=An%20individual's%20personal%20information%20can,by%20cybersecurity%20researcher%20Privacy%20Affairs.

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] Lazarus, Ari, How fast will identity thieves use stolen info?, Military Consumer (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info

[10] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

that they have already been the victim of identity theft (i.e. fraudulent acquisition and use of another person's Personal Information)—it does not prevent identity theft.

59. As a direct and proximate result of the Data Breach, Plaintiff and the Breach Victims have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and the Breach Victims now have to take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

60. Plaintiff and the Breach Victims have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

i. Trespass, damage to and theft of their personal property including Personal Information;

ii. Improper disclosure of their Personal Information;

iii. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals and having been already misused;

iv. Damages flowing from Defendant untimely and inadequate notification of the data breach;

v. Loss of privacy suffered as a result of the data breach;

vi. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

vii. Ascertainable losses in the form of deprivation of the value of customers' personal information for which there is a well-established and quantifiable national and international market;

viii. The loss of use of and access to their credit, accounts, and/or funds;

ix. Damage to their credit due to fraudulent use of their Personal Information; and

x. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

61. Moreover, Plaintiff and Breach Victims have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards.

62. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiff and Breach Victims two years of identity theft repair and monitoring services. Two years of identity theft and repair and monitoring is woefully inadequate to protect Plaintiff and Breach Victims from a lifetime of identity theft risk and does nothing to reimburse Plaintiff and Breach Victims for the injuries they have already suffered.

CLASS ALLEGATIONS

63. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

64. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23. The requirements of Federal Rule of Civil Procedure 23 (a) and 23(b)(3), Plaintiff asserts all claims on behalf of a Nationwide Class, as defined as follows: **All persons whose Personal Information was compromised by the September 21, 2023 Data Breach, including all who were sent a notice of the Data Breach.**

65. Excluded from the Class is Defendant, its legal representatives, assignees, and successors, and any entity in which the Defendant has controlling interest. Also, excluded from the Class is the judge to whom this case is assigned, the Judge's immediate family, and Plaintiff's counsel and their employees. Plaintiff reserves the right to amend the above-stated class definitions based on facts learned in discovery, as well as adding subclasses as the Court sees fit.

66. Alternatively, Plaintiff Proposes the following subclasses by state or groups of states, defined as follows: **Statewide [Name of State] Class: All residents of [name of State] whose Personal Information was compromised by the Data Breach.**

67. The proposed Nationwide Class, or alternatively, the separate Statewide Class (collectively, the "Class" as used in this sub-section) meet the requirements under Rule of Civil Procedure 23 (a), (b)(1), (b)(2), (b)(3), and (c)(4).

68. **Numerosity:** The proposed Class is so numerous that joinder all members is impracticable.

69. **Commonality and Predominance:** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual Class Members. These common legal and factual questions include, but are not limited to, the following:

xi. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's Personal Information;

xii. Whether Defendant failed to protect Plaintiff's and the Class's Personal Information;

xiii. Whether Defendant's email and computer systems and data security practices used to protect Plaintiff's and the Class's Personal Information violated federal and state laws, and/or Defendant's other duties;

xiv. Whether Defendant violated the data security statutes and data breach notification statutes applicable to Plaintiff and the Class;

xv. Whether Defendant failed to notify Plaintiff and members of the Class about the Data Breach expeditiously and without unreasonable delay after the Data Breach was discovered;

xvi. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Breach Victims' Personal Information properly and as promised;

xvii. Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Class's Personal Information;

xviii. Whether Defendant entered into implied contracts with Plaintiff and the members of the Class that included contract terms requiring Defendant to protect the confidentiality of Personal Information and have reasonable security measures;

xix. Whether Defendant violated the consumer protection statutes, data breach notification statutes, and state privacy statutes applicable to Plaintiff and the Class;

xx. Whether Defendant failed to notify Plaintiff and Breach Victims about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

xxi. Whether Defendant's conduct described herein constitutes a breach of their implied contracts with Plaintiff and the Class;

xxii. Whether Plaintiff and the members of the Class are entitled to damages as a result of Defendant's wrongful conduct;

xxiii. What equitable relief is appropriate to redress Defendant's wrongful conduct; and

xxiv. What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by members of the Class.

70. **Typicality:** Plaintiff's claims are typical of the Class and within each subclass and are based on the same facts, legal theories and/or primary rights of all Class members, because Plaintiff and each Class member were identically injured in by having their Personal Information accessed by unauthorized persons as a direct result of Defendant's Data Breach.

71. **Superiority:** The class action procedure is also superior to individual lawsuits due to the massive volume of potential individual lawsuits and the similarities that persist in each Class member's claims when compared against the predicted amount of recovery per Class member. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if members of the Class could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

72. **Adequacy:** Plaintiff will adequately and fairly protect the interests of the Class. She has retained counsel experiences in class action litigation. Neither Plaintiff nor her counsel have any interest that might cause them to not vigorously pursue this action in the Class's best interest.

73. Plaintiff and her counsel anticipate that notice to the proposed Class will be effectuated by mailing notice to each and every individual that Defendant has already sent a Notice regarding the Data Breach to on or around September 5,

2023, whose Personal Information was potentially accessed by unauthorized users during the Data Breach.

74. This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, Defendant are still in possession of Personal Information of Plaintiff and the Class, and Defendant's systems are still vulnerable to attack—one standard of conduct is needed to ensure the future safety of Personal Information in Defendant's possession.

75. This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Plaintiff and the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

FIRST CAUSE OF ACTION

(Negligence – *By Plaintiff on behalf of the Class, against Defendant and Does 1-50*)

76. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

77. Defendant solicited, gathered, and stored the Personal Information of Plaintiff and the Class.

78. Defendant knew, or should have known, of the risks inherent in collecting and storing the Personal Information of Plaintiff and the Class and the importance of adequate security.

79. Defendant were well aware of the fact that hackers routinely attempted to access Personal Information without authorization. Defendant also knew about numerous, well-publicized data breaches wherein hackers stole the Personal Information from companies, including its own company, who held or stored such information.

80. Defendant owed duties of care to Plaintiff and the Class whose Personal Information was entrusted to it. Defendant's duties included the following:

i. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Personal Information in its possession;

ii. To protect the Personal Information in its possession using reasonable and adequate security procedures and systems;

iii. To adequately and properly train its employees to avoid phishing emails;

iv. To use adequate email security systems, including DMARC enforcement and Sender Policy Framework enforcement, to protect against phishing emails;

v. To adequately and properly train its employees regarding how to properly and securely transmit and store Personal Information;

vi. To train its employees not to store Personal Information in their email inboxes longer than absolutely necessary for the specific purpose that it was sent or received;

vii. To implement processes to quickly detect a data breach, security incident, or intrusion; and

viii. To promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their Personal Information.

81. Because Defendant knew that a security incident, breach or intrusion upon its systems would potentially damage thousands of its current and/or former patients and employees, including Plaintiff and Class members, it had a duty to adequately protect their Personal Information.

82. Defendant owed a duty of care not to subject Plaintiff and the Class to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices

83. Defendant knew, or should have known, that its security practices and computer systems did not adequately safeguard the Personal Information of Plaintiff and the Class. Defendant breached its duties of care by failing to provide fair, reasonable, or adequate computer systems and security practices to safeguard the Personal Information of Plaintiff and the Class.

84. Defendant breached their duties of care by failing to provide prompt notice of the Data Breach to the persons whose personal information was compromised.

85. Defendant acted with reckless disregard for the security of the Personal Information of Plaintiff and the Class because Defendant knew or should have known that their computer systems and data security practices were not adequate to safeguard the Personal Information that it collected and stored, which hackers were attempting to access.

86. Defendant acted with reckless disregard for the rights of Plaintiff and the Class by failing to provide prompt and adequate notice of the data breach so that they could take measures to protect themselves from damages caused by the fraudulent use of Personal Information compromised in the Data Breach.

87. Defendant had a special relationship with Plaintiff and the Class. Plaintiff's and the Class's willingness to entrust Defendant with their personal information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems (and the Personal Information stored on them) and to implement security practices to protect the Personal Information that it collected and stored from attack.

88. Defendant own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Personal Information. Defendant's misconduct included failing to:

ix. Secure its employees' email accounts;

x. Secure access to its servers;

xi. Comply with current industry standard security practices;

xii. Encrypt Personal Information during transit and while stored on Defendant's systems;

xiii. Properly and adequately train their employees on proper data security practices;

xiv. Implement adequate system and event monitoring;

xv. Implement the systems, policies, and procedures necessary to prevent hackers from accessing and utilizing Personal Information transmitted and/or stored by Defendant;

xvi. Undertake periodic audits of record-keeping processes to evaluate the safeguarding of Personal Information;

xvii. Develop a written records retention policy that identifies what information must be kept and for how long;

xviii. Destroy all discarded employee information, including information on prospective employees, temporary workers, subcontractor, and former employees;

xix. Secure Personal Information and limit access to it to those with a legitimate business need;

xx. Employ or contract with trained professionals to ensure security of network servers and evaluate the systems used to manage e-mail, Internet use, and so forth;

xxi. Avoid using Social Security numbers as a form of identification; and

xxii. Have a plan ready and in position to act quickly should a theft or data breach occur.

89. Defendant also had independent duties under federal and state law requiring them to reasonably safeguard Plaintiff's and the Class's Personal Information and promptly notify them about the Data Breach.

90. Defendant breached the duties they owed to Plaintiff and Class members in numerous ways, including:

xxiii. By creating a foreseeable risk of harm through the misconduct previously described;

xxiv. By failing to implement adequate security systems, protocols and practices sufficient to protect their Personal Information both before and after learning of the Data Breach;

xxv. By failing to comply with the minimum industry data security standards before, during, and after the period of the Data Breach; and

xxvi. By failing to timely and accurately disclose that the Personal Information of Plaintiff and the Class had been improperly acquired or accessed in the Data Breach.

91. But for Defendant wrongful and negligent breach of the duties it owed Plaintiff and the Class members, their Personal Information either would not have been compromised or they would have been able to prevent some or all of their damages.

92. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of further harm.

93. The injury and harm that Plaintiff and Class members suffered (as alleged above) was reasonably foreseeable.

94. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligent conduct.

95. Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION

(Negligence Per Se – *By Plaintiff on behalf of the Class, against Defendant and Does 1-50*)

96. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

97. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the Personal Information of Plaintiff and the Class.

98. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by

businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

99. Defendant solicited, gathered, and stored the Personal Information of Plaintiff and the Class as part of its business of manufacturing, selling, and installing gutter protection systems, which affects commerce.

100. Defendant violated the FTCA by failing to use reasonable measures to protect the Personal Information of Plaintiff and the Class and not complying with applicable industry standards, as described herein.

101. Defendant breached its duties to Plaintiff and the Class under the FTCA and other state data security and privacy statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Breach Victim's Personal Information.

102. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

103. Plaintiff and the Class are within the class of persons that the FTCA was intended to protect.

104. The harm that occurred as a result of the Data Breach is the type of harm the FTCA, the state data breach privacy statutes were intended to guard against.

105. Defendant breached its duties to Plaintiff and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Personal Information.

106. Defendant breached their duties to Plaintiff and the Class by negligently and unreasonably delaying and failing to provide notice expeditiously and/or as soon as practicable to Plaintiff and the Class of the Data Breach.

107. Defendant's violation of the FTCA, state data security statutes, and/or the state data breach notification statutes constitute negligence per se.

108. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach by, inter alia, having to spend time reviewing their accounts and credit reports for unauthorized activity; spend time and incur costs to place and re-new a "freeze" on their credit; be inconvenienced by the credit freeze, which requires them to spend extra time unfreezing their account with each credit bureau any time they want to make use of their own credit; and becoming a victim of identity theft, which may cause damage to their credit and ability to obtain insurance, medical care, and jobs.

109. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

THIRD CAUSE OF ACTION

(Breach of Fiduciary Duties– *By Plaintiff on behalf of the Class, against Defendant and Does 1-50*)

110. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

111. A relationship existed between Plaintiff and Class Members and Defendant in which Plaintiff and the Class put their trust in Defendant to protect their Personal Information. Defendant accepted this duty and obligation when it received Plaintiff and the Class Members' Personal Information.

112. Plaintiff and the Class Members entrusted their Personal Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Personal Information for

business purposes only, and refrain from disclosing their Personal Information to unauthorized third parties.

113. Defendant knew or should have known that the failure to exercise due care in the collecting, storing, and using of individual's Personal Information involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

114. Defendant's fiduciary duty required it to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff and the Class's information in Defendant's possession was adequately secured and protected.

115. Defendants also had a fiduciary duty to have procedures in place to detect and prevent improper access and misuse of Plaintiff's and the Class's Personal Information. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Defendant was entrusted with Plaintiff and the Class's Personal Information.

116. Defendant breached its fiduciary duty that it owed Plaintiff and the Class by failing to case in good faith, fairness, and honesty; by failing to act with the highest and finest loyalty; and by failing to protect the Personal Information of Plaintiff and the Class Members.

117. Defendant's breach of fiduciary duties was a legal cause of damages to Plaintiff and the Class.

118. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred, and the Data Breach contributed substantially to producing the damage to Plaintiff and the Class.

119. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and the Class are entitled to actual, consequential, and nominal damages and injunctive relief, with amounts to be determined at trial.

FOURTH CAUSE OF ACTION

(Breach of Confidence – *By Plaintiff on behalf of the Class, against Defendant and Does 1-50*)

120. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

121. Defendant was fully aware of the confidential nature of the Personal Information of Plaintiff and Class Members that it was provided.

122. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by promises and expectations that Plaintiff and Class Members' Personal Information would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

123. Plaintiff and Class members provided their respective Personal Information to Defendant's clients, and by proxy to Defendant, with the explicit and implicit understandings that Defendant would protect and not permit the Personal Information to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

124. Plaintiff and Class Members provided their respective Personal Information to Defendant's clients, and by proxy to Defendant, with the explicit

and implicit understandings that Defendant would take precautions to protect their Personal Information from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting their networks and data systems.

125. Defendant voluntarily received, in confidence, Plaintiff and Class members' Personal Information with the understanding that the Personal Information would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

126. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, inter alia, not following best information security practices to secure Plaintiff and Class Members' Personal Information, Plaintiff and Class Members' Personal Information was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Plaintiff and Class Members' confidence, and without their express permission.

127. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class members have suffered damages as alleged herein.

128. But for Defendant's failure to maintain and protect Plaintiff and Class Members' Personal Information in violation of the parties' understanding of confidence, their Personal Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the misuse of Plaintiff and Class members' Personal Information, as well as the resulting damages.

129. The injury and harm Plaintiff and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's

unauthorized misuse of Plaintiff and Class members' Personal Information. Defendant knew its data systems and protocols for accepting and securing Plaintiff and Class Members' Personal Information had security and other vulnerabilities that placed Plaintiff and Class members' Personal Information in jeopardy.

130. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will suffer injury, as alleged herein, including but not limited to (a) actual identity theft; (b) the compromise, publication, and/or theft of their Personal Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Personal Information; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their Personal Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Class Members' Personal Information in their continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (g) the diminished value of Plaintiff and Class Members' Personal Information.

FIFTH CAUSE OF ACTION

(Breach of Implied Contract – *By Plaintiff on behalf of the Class, against Defendant and Does 1-50*)

131. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

132. By requiring Plaintiff and the Class Members Personal Information to engage in or settle a litigation suit, Defendant entered into an implied contract in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff and Class Members' Personal Information. In return, Defendant engaged in and/or settled Plaintiff and Class Members' suits.

133. Based on this implicit understanding, Plaintiff and the Class accepted Defendant's offers and provided Defendant with their Personal Information.

134. Plaintiff and Class members would not have provided their Personal Information to Defendant had they known that Defendant would not safeguard their Personal Information, as promised.

135. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

136. Defendant breached the implied contracts by failing to safeguard Plaintiff and Class Members' Personal Information.

137. Defendant also breached the implied contracts when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC. These acts and omissions included (i) representing, either expressly or impliedly, that it would maintain adequate data privacy and security practices and procedures to safeguard the Personal Information from unauthorized disclosures, releases, data breaches, and theft; (ii) omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class's Personal Information; and (iii) failing to disclose to the nursing programs and the Class at the time they provided their Personal Information that Defendant's data security system and protocols failed to meet applicable legal and industry standards.

138. The losses and damages Plaintiff and Class members sustained were the direct and proximate result of Defendant's breach of the implied contract with Plaintiff and Class Members.

SIXTH CAUSE OF ACTION

(Invasion of Privacy – *By Plaintiff on behalf of the Class, against Defendant and Does 1-50*)

139. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

140. Plaintiff and Class Members had a legitimate expectation of privacy regarding their Personal Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

141. Defendant owed a duty to Plaintiff and Class Member to keep their Personal Information confidential.

142. Defendant affirmatively and recklessly disclosed Plaintiff and Class Members' Personal Information to unauthorized third parties.

143. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiff and Class Members' Personal Information is highly offensive to a reasonable person.

144. Defendant's reckless and negligent failure to protect Plaintiff and Class Members' Personal Information constitutes an intentional interference with Plaintiff and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

145. In failing to protect Plaintiff and Class Members' Personal Information, Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

146. Because Defendant failed to properly safeguard Plaintiff and Class Members' Personal Information, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

147. Defendant knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

148. As a proximate result of Defendant's acts and omissions, Plaintiff and the Class Members' private and sensitive Personal Information was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

149. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Personal Information are still maintained by Defendant with their inadequate cybersecurity system and policies.

150. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard Plaintiff and the Class's Personal Information.

151. Plaintiff, on behalf of herself and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff and Class Members' Personal Information.

152. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

/ / /

/ / /

SEVENTH CAUSE OF ACTION

(Injunctive Relief/Declaratory Relief – *By Plaintiff on behalf of the Class, against Defendant and Does 1-50*)

153. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

154. Plaintiff and members of the Class entered into an implied contract that required Defendant to provide adequate security for the Personal Information it collected from Plaintiff and the Class.

155. Defendant owe a duty of care to Plaintiff and the members of the Class that requires them to adequately secure Personal Information.

156. Defendant still possess Personal Information regarding Plaintiff and members of the Class.

157. Since the Data Breach, Defendant has announced few if any changes to their data security infrastructure, processes or procedures to fix the vulnerabilities in their computer systems and/or security practices which permitted the Data Breach to occur and go undetected for months and, thereby, prevent further attacks.

158. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class. In fact, now that Defendant's insufficient information security is known to hackers, the Personal Information in Defendant possession is even more vulnerable to cyberattack.

159. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the Class are at risk of additional or further harm due to the exposure of their Personal Information and Defendant's failure to address the security failings that lead to such exposure.

160. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

161. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

xxvii. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

xxviii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

xxix. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

xxx. Ordering that Defendant's segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

xxxi. Ordering that Defendant cease transmitting Personal Information via unencrypted email;

xxxii. Ordering that Defendant cease storing Personal Information in email accounts;

xxxiii. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

xxxiv. Ordering that Defendant conduct regular database scanning and securing checks;

xxxv. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

xxxvi. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Complaint.

Dated:

EMPLOYEE JUSTICE LEGAL GROUP P.C.

By: Saima Ali Gipson
Kaveh Elihu, Esq.
Saima Ali Gipson, Esq.
Attorney for Plaintiff and Proposed Counsel for the Classes